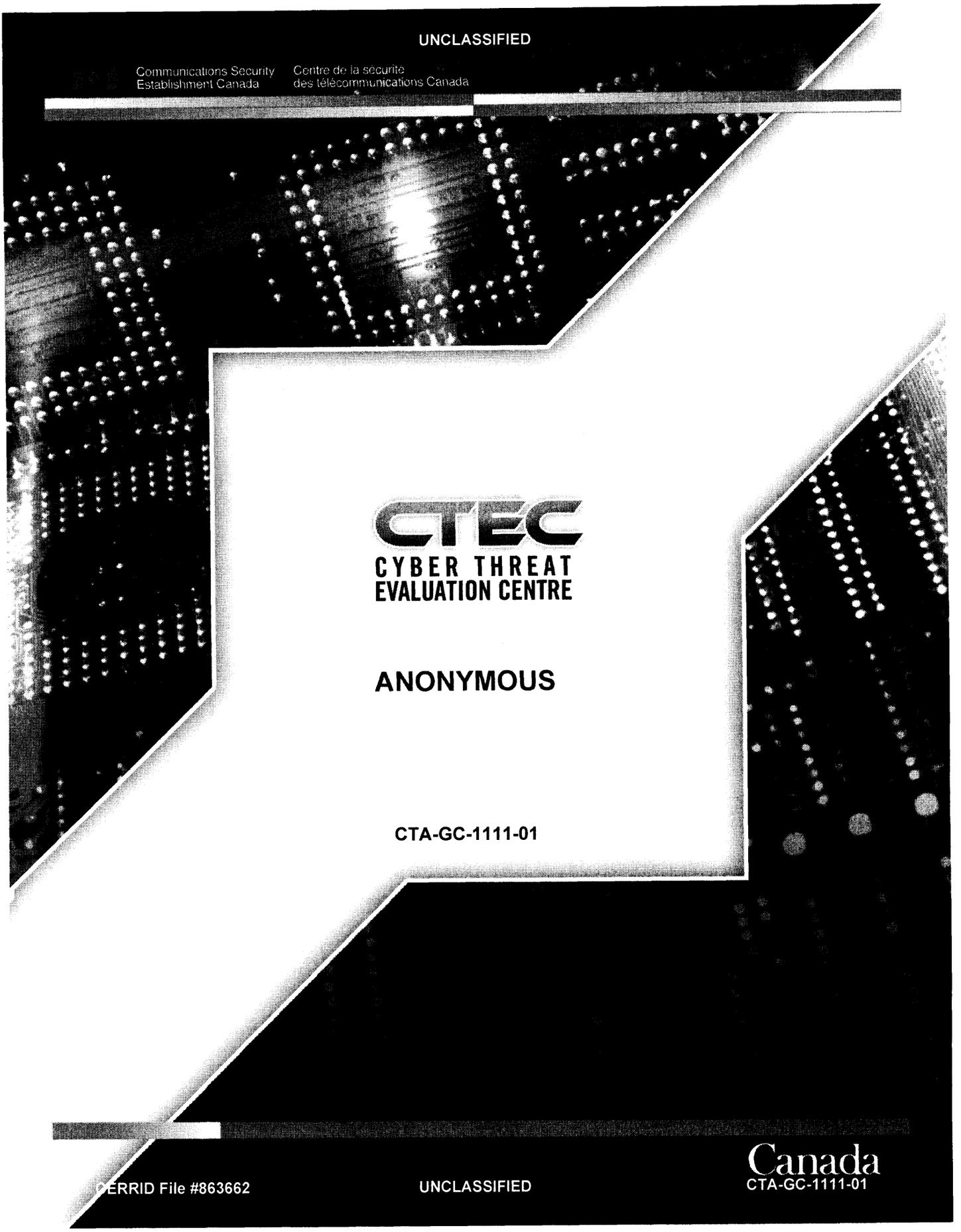
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



CTEC
CYBER THREAT EVALUATION CENTRE

ANONYMOUS

CTA-GC-1111-01

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2

OVERVIEW 3

STRUCTURE 3

CHOOSING TARGETS 4

PAST TARGETS/BEHAVIOUR 4

CANADA 8

TRADECRAFT 10

MITIGATION 12

The intended audience for this report is GC IT decision makers, security officers and technical practitioners.

EXECUTIVE SUMMARY

This report provides an overview of the hacktivist group, "Anonymous" and contains: information on its organizational structure, tradecraft, and targets; the threat to GC systems; and, CTEC's prevention and mitigation advice.

- "Anonymous" targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on:
  - civil rights (e.g. oppressive government regimes); and,
  - information accessibility (e.g. perceived government-mandated Internet censorship).
- Based on a view of previous targeting by "Anonymous", Government of Canada systems could be targeted due to:
  - government legislative initiatives (e.g. *Copyright Modernization Act*); and,
  - political initiatives that may result in activist opposition (e.g. environmental or social issues).
- Specific targets are chosen in a variety of ways, including:
  - through online polls following discussions in Internet Relay Chats (IRC[1]);
  - opposition to "Anonymous'" campaigns, such as the ongoing "Operation Anti-Security";
  - as a response to provocations made by companies, governments or other hacking groups; and,
  - as targets of opportunity, following searches for vulnerable systems.
- "Anonymous" uses a number of capabilities against its targets. These include, but may not be limited to Distributed Denial of Service (DDoS[2]), password cracking, SQL injections[3], and malware (virus) deployments.
- Canadian organizations have been both direct and indirect targets of "Anonymous" activity, for example:
  - the Toronto Police Service website was hacked in 2011, likely in response to "Occupy Toronto" camp evictions;
  - Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and
  - Subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian federal departments to access STRATFOR databases were published.
- Although "Anonymous" leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against "Anonymous" exploits. The majority of these exploits are not "zero-day[4]". Please refer to the "Mitigation" section and Annex 1 for details.

[1] IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.
[2] A denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.
[3] SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application to change the database content or to dump database information to the attacker.

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their own agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or "hacktivists," who pose a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship, and in support of worldwide activist movements.

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g.: Anon-ops[5], LulzSec[6]) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, "TeaMp0isoN" and "People's Liberation Front" are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. In addition, the Anonymous movement has inspired copycat actions from other hacktivist groups, such as LulzRaft[7].

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several "unofficial" spokespeople[8], Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts. In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)[9] onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

---

[4] Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.
[5] Anon-ops provides communications for Anonymous' announcements.
[6] LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.
[7] LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the website for the Conservative Party of Canada and for accessing private information about the party's donors. They have also been linked to web defacement of the website of Calgary-based energy company, Husky Energy.
[8] Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary,") Barrett Brown, etc. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-uk-police/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.
[9] According to open source, LOIC is an open source network stress testing application which performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly utilized and documented methods of selecting targets are:

- through consensus among Anons using online polls. Following a discussion on an Internet Relay Chat (IRC), an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks;

- as a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary[10]), against the group as a whole, or against the principles to which Anonymous adheres; and,

- to "expose" poor security practices: for instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity.

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"); which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Its hacktivism efforts have recently been concentrated on the various Occupy[11] movements, on protesting Internet censorship and Internet filtering, on protesting against oppressive regimes, and on supporting WikiLeaks.

[10] HBGary Federal is a technology security company who was working with the FBI to unmask members of Anonymous. In February 2011, the CEO Aaron Barr revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website, stole and publicly released the company's documents and emails.
[11] According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

These campaigns include:

2008:

PROJECT CHANOLOGY (worldwide):

- *Action:* DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.
- *Reason:* The Church of Scientology was attempting to restrict access to information which it found embarrassing and was readily available on the Internet.

2009:

ANONYMOUS IRAN (Iran):

- *Action:* Creation of an Iranian Green Party Support site, Anonymous Iran, to provide covert resources and event updates to Iranian protestors during government-imposed Internet information censorship.
- *Reason:* To provide support to Iranian protestors against a regime perceived to be corrupt.

OPERATION DIDGERIDIE (Australia):

- *Action:* a DDoS attack was launched against the Australian Prime Minister's website.
- *Reason:* To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:

OPERATION TITSTORM (Australia):

- *Action:* DDoS attack against the Australian Parliament's website and web defacement of the Prime Minister's website.
- *Reason:* To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

OPERATION PAYBACK/OPERATION SONY (worldwide):

- *Action:* DDoS attacks against Sony PlayStation websites.
- *Reason:* To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications[12].

[12] For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

OPERATION AVENGE ASSANGE (USA):

- *Action:* DDoS attacks against the Amazon, Paypal, Mastercard and Visa websites.
- *Reason:* To show support for WikiLeaks and to protest against its founder's arrest.

OPERATION ZIMBABWE (Zimbabwe):

- *Action:* DDoS attacks against the Government of the Republic of Zimbabwe's websites.
- *Reason:* To protest against censorship of WikiLeaks documents.

2011:

OPERATION TUNISIA (Tunisia):

- *Action:* DDoS attack on the Government of Tunisia's websites.
- *Reason:* To protest against Internet censorship; and to support the Arab Spring[13].

OPERATION SYRIA (Syria):

- *Action:* Web defacement of Syrian Defence Ministry website.
- *Reason:* To support the Arab Spring (Syrian uprising).

OPERATION EGYPT (Egypt):

- *Action:* DDoS attack against the Government of Egypt's website and the website of the National Democratic Party. Also released the names and passwords of email addresses of government officials.
- *Reason:* To support the Arab Spring (Egyptian revolution).

HBGARY FEDERAL (USA):

- *Action:* The defacement of HBGary's website, the deletion of company files and the publication of 68,000 employee emails.
- *Reason:* HBGary official provoked Anonymous by threatening to expose information about the group.

BANK OF AMERICA (USA):

- *Action:* The release of sensitive Bank of America documents online which allegedly prove cases of corruption and fraud at the bank.
- *Reason:* To protest in support of allegations of corruption and fraud within the US banking system.

[13] The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

OPERATION MALAYSIA (Malaysia):

- *Action:* DDoS attacks on 91 Government of Malaysia's websites.
- *Reason:* In response to the Malaysian government's censorship of sites like the Pirate Bay[14] and WikiLeaks.

OCCUPY WALL STREET (USA):

- *Action:* DDoS attacks on the Oakland Police Department website and the St. Louis mayor's website.
- *Reason:* To protest evictions of protestors from Occupy sites; in support of the worldwide Occupy movement.

OPERATION MAYHEM (USA):

- *Action:* The release of Guy Fawkes virus on Facebook.
- *Reason:* To protest the *Stop Online Piracy Act*[15], perceptions of police violence towards protestors in Occupy movements, and any opposition to Anonymous activities.

COX COMMUNICATIONS (USA):

- *Action:* Domain name system (DNS) servers taken offline, removing Internet access for clientele in most of southwest America.
- *Reason:* To protest Cox Communications' attempted regulation of customer's data usage quota.

OPERATION BLACKOUT (USA):

- *Action:* In November, Anonymous threatened action against the US government.
- *Reason:* To protest against the *Stop Online Piracy Act*.

STRATFOR (worldwide):

- *Action:* STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. 200 gigabytes of data were stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including governments and military departments). Anonymous planned to donate to charities using the stolen credit card information.

---

[14] The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.
[15] The *Stop Online Piracy Act* is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

- *Reason:* Following the HB Gary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the U.S. and elsewhere.[16]"

Ongoing:

OPERATION ANTISEC (NATO, Tunisia, Brazil, Australia, USA, Turkey, UK, and other countries):

- *Action:*
  - In USA: DDoS attacks against the Central Intelligence Agency's (CIA) website; the US Senate website was hacked, and information about its internal server structure was released.
  - In UK: DDoS attacks against the Serious Organised Crime Agency's (SOCA) website.
- *Reason:* The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA

Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations.

Government of Canada:

STRATFOR (December 2011):

- The federal government has been an indirect target of anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees[17].

Municipal Governments:

TORONTO (November 2011):

- Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto

[16] For the full explanation, please refer to Barret Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27-million-stratfor-emails-were-hacked.
[17] CTEC has provided mitigation to employees of the affected departments.

Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:

OPERATION GREEN RIGHTS/ PROJECT TARMAGGEDON:

- In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline, and the Alberta Tar Sands project. Those targeted have included Canadian Oil Sands Ltd, Imperial Oil, Syncrude, and Suncor.

Future Activity

Although it is impossible to fully predict Anonymous' behaviour, based on prior targeting, there are a few government bills that would direct Anonymous' attention towards the Government of Canada.

Copyright Modernization Act:

- As a part of this bill, ISPs would be responsible for sending notices from copyright holders to Internet users alleged to have participated in illicit downloading and file-sharing online. The ISPs would also be required to retain records which establish the identity of the subscriber and disclose it in court if necessary. (Comment: This could be seen by Anonymous as an attempt to limit consumer rights. Previous protests against government-issued copyright laws in Australia and the USA resulted in Anonymous launching DDoS attacks on Australian government websites and the US Copyright Office.)

Lawful Access Package:

- The government's announcement to reintroduce Lawful Access legislation[18] that would require telecommunications companies, including ISPs to ensure intercept capabilities on their network. ISPs would also be required to disclose certain information on persons of interest to law enforcement authorities without a warrant under specific circumstances. (Comment: This could be seen by Anonymous as a violation of privacy. Similar perceptions have prompted Anonymous to take action against Facebook[19].)

[18] This legislation will be similar to the previous Bill C-50, Bill C-51 and Bill C-52.
[19] Operation Facebook was launched on November 5th, 2011 because Anonymous believes that "Facebook is the opposite of the Antisec cause."

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous includes a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

Open Source resources:

DoS/DDoS:

Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

1) LOIC:

Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which would then disrupt the service of the victim's host. However, since LOIC could reveal the IP addresses of its users, it's traceability has prompted Anonymous to find other means of attacks.

2) Apache Killer:

The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability which allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)[20]. It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

Anonymous-developed tools:

DoS/DDoS via SQL Injections:

#RefRef:

Anonymous developed and released a Perl DDoS tool in September, #RefRef, that exploits SQL[21] vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline.

---

[20] For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

[21] An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

#RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes virus:
Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes[22] virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known anti-malware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:
Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HB Gary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

[22] Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

MITIGATION

Since Anonymous has a wide range of targets, it is difficult to measure which vulnerabilities are most frequently exploited by the group. However, as noted, the threats leveraged are generally limited to open source or well-known vulnerabilities. As a result, strong IT security practices will go a long way to defending against an Anonymous cyber threat.

In addition to best practices, including the implementation of CTEC's "Top 35 Mitigation Actions", the following mitigation is available for some of the tradecraft[23] specifically noted above:

1. DoS/DDoS attacks.
    a. Use network segmentation and segregation into security zones to protect high value assets using routers to spot and drop DDoS connections. For more information, please refer to number 16 of the "Top 35 Mitigation Actions" in Annex 1.
    b. If the DDoS is pointed at a specific IP, the target site could be blackholed. This typically requires working with upstream network providers to forward malicious traffic to a non-existent network interface, where the offending traffic will be dropped.
    c. In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

2. "Apache Killer."
    a. Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher. Also, please refer to the "Top 35 Mitigation Actions" numbers 1 and 2.

3. "#RefRef."
    a. Webcode should be hardened[24] against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users.

Please see CTEC report "Government of Canada Top 35 Mitigation Actions, January 2012" for further information.

---

[23] Security analysts are still undergoing analysis on the Guy Fawkes virus; as such, we are unable to provide mitigation at this time. In addition, since URGE is not a hacking tool, there does not appear to be any mitigation actions provided at this time.
[24] Hardening minimises access between the public facing HTTP server and the SQL database. It also validates requests sent by external clients to the HTTP server.